Law Offices
FOLEY & LARDNER
3000 K Street, N.W., Suite 500
P.O. Box 25696
Washington, D.C. 20007-8696
(202) 672-5300

jc525 U.S. PTO
09/303561
05/03/99

TO: Assistant Commissioner for Patents
Box Patent Applications
Washington D.C. 20231

jc408 U.S. PTO
05/03/99

Attorney Docket No.088941-0129
(must include alphanumeric codes if no inventors named)

UTILITY PATENT APPLICATION TRANSMITTAL
(new nonprovisional applications under 37 CFR 1.53(b))

Transmitted herewith for filing is the patent application of:

INVENTOR(S): Takuya MORISHITA

TITLE: SYSTEM AND METHOD FOR PREVENTING ILLEGAL USE OF SOFTWARE

In connection with this application, the following are enclosed:

APPLICATION ELEMENTS:

XX Specification - 17 TOTAL PAGES
(preferred arrangement:)
- -Descriptive Title of the Invention
- -Cross Reference to Related Applications
- -Statement Regard Fed sponsored R&D
- -Reference to Microfiche Appendix
- -Background of the Invention
- -Brief Summary of the Invention
- -Brief Description of the Drawings (if filed)
- -Detailed Description
- -Claim(s)
- -Abstract of the Disclosure

XX Drawings - Total Sheets 5

XX Declaration and Power of Attorney - Total Sheets 2

XX Newly executed (original or copy)

___ Copy from a prior application (37 CFR 1.63(d))
(relates to continuation/divisional boxes completed) - NOTE: Box below

____ DELETION OF INVENTOR(S) - Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

___ Incorporation By Reference (useable if copy of prior application Declaration being submitted)

The entire disclosure of the prior application, from which a COPY of the oath or declaration is supplied as noted above, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

___ Microfiche Computer Program (Appendix)

___ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
- ___ Computer Readable Copy
- ___ Paper Copy (identical to computer copy)
- ___ Statement verifying identify of above copies

ACCOMPANYING APPLICATION PARTS

XX Assignment Papers (cover sheet & document(s))
____ 37 CFR 3.73(b) Statement (when there is an assignee)
____ English Translation Document (if applicable)
XX Information Disclosure Statement(IDS) with PTO-1449. 3 Copies of IDS Citations
____ Preliminary Amendment
XX Return Receipt Postcard (MPEP 503)

____ Small Entity Statement(s)
__ Statement file in prior application, status still proper and desired.
_XX_ Certified Copy of Priority Document(s) with Claim of Priority (if foreign priority is claimed).
_XX_ OTHER: Check for $800.00

If a **CONTINUING APPLICATION**, **check appropriate box and supply the requisite information:**
__ Continuation __ Divisional __ Continuation-in-part (CIP) of prior application Serial No. __.

__ Amend the specification by inserting before the first line the following sentence: --This application is a __ continuation, __ divisional or __ continuation-in-part of application Serial No. __, filed __.--

CORRESPONDENCE ADDRESS:
Foley & Lardner Address noted above.
Telephone: (202) 672-5300
Fax Number: (202) 672-5399

FEE CALCULATIONS: (Small entity fees indicated in parentheses.)

(1) For	(2) Number Filed	(3) Number Extra	(4) Rate	(5) Basic Fee $760 ($380)
Total Claims	9 - 20 =	0	x $18 (x $9)	0.00
Independent Claims	3 - 3 =	0	x $78 (x $39)	0.00
Multiple Dependent Claims			$260 ($130)	0.00
Assignment Recording Fee per property			$40	40.00
			TOTAL FEE:	$800.00

METHOD OF PAYMENT:
A check in the amount of the above TOTAL FEE is attached. If payment is enclosed, this amount is believed to be correct; however, the Commissioner is hereby authorized to charge any deficiency or credit any overpayment to Deposit Account No. 19-0741.

Respectfully submitted,

Date: May 3, 1999
Docket No.: 088941-0129

for/ Phillip J. Articola Reg. No. 38,819
David A. Blumenthal
Reg. No. 26,257

SYSTEM AND METHOD FOR PREVENTING ILLEGAL USE OF SOFTWARE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system and method for preventing illegal use of software, in particular, a system for preventing an illegal user from decrypting secret information stored in an IC card or the like, which is distributed to a general user.

This application is based on Patent Application No. Hei 10-125619 filed in Japan, the contents of which are incorporated herein by reference.

2. Description of the Related Art

When An IC card for medical use stores software including secret information concerning patients, it is necessary to prevent a third party from decrypting such secret information and illegally using it.

For example, there are two conventional systems used for preventing illegal use of software:

Fig. 5 is a diagram showing the first conventional system for keeping the control program in the operating system (OS) for a microcomputer (i.e., a semiconductor integrated circuit) secret (refer to Japanese Patent Application, First Publication, No. Hei 8-185361).

In Fig. 5, microcomputer 1 includes a system memory (i.e., storage means) 2, a rewritable and nonvolatile memory, in which a control program such as the Kernel in the OS is stored. The system memory 2 stores (i) decrypting key FK used for decrypting data such as an encrypted control program based on a specific decrypting algorithm, and

(ii) decrypting-process information FT which includes a program for executing the decrypting algorithm by using the decrypting key FK. The decrypting key FK and decrypting-process information FT are stored in the system memory 2; thus, a user can rewrite this data as the user chooses.

There are two types of the applicable cryptosystems, a symmetrical cryptosystem in which encrypting and decrypting operations are performed using the same key, and an asymmetrical cryptosystem in which encrypting and decrypting operations are performed using different keys. Either system can be used in the system of Fig. 5. In the encrypting and decrypting operations, a reversible operation such as exchange or inversion in a specific bit sequence is controlled using a key.

The microcomputer 1 also comprises input/output circuit 3 for inputting or outputting data via external bus Bg, and RAM 4 for storing specific data input from the input/output circuit 3. The microcomputer 1 further comprises CPU (central processing unit) 5 which controls all the operations of the microcomputer 1. Decoding means FS in this system consists of CPU 5, decrypting key FK, and decrypting-process information FT. The system memory 2, input/output circuit 3, RAM 4, and CPU 5 are connected with each other via an internal bus 6.

The conventional system (for preventing illegal use of software) having the above structure employs the following method for protecting secret information from an illegal user.

In this system, a function of CPU 5 for protecting commands and data is used. The system memory 2 can be accessed only in the supervisor mode. Therefore, generally, secret information stored in the system memory 2 cannot be retrieved by a general user.

The second conventional system for preventing illegal use employs a dedicated

device or means for storing secret information, and has the function of physically destroying the dedicated device when an illegal user tries to physically analyze the system.

However, the above first and second illegal-use preventing systems have the following problems.

The problem caused by the first system is that secret information cannot be completely protected by the relevant software. The reason is that the secret-information protecting means in the first system only inhibits an access in a mode other than the supervisor mode; thus, if an illegal user tries to perform an analysis using a software debugger which is operated in the supervisor mode, the protection of secret information is ineffective.

The problem caused by the second system is that if such a dedicated means is wholly constructed using software, secret information itself must be stored in a general file storage device. In this case, the secret information can also be stored in another file storage device as a backup copy. Therefore, if an illegal user stores backup data of secret information in another file storage device in advance, it is easy to restore the backup data even if secret information stored in the main file storage system is destroyed.

SUMMARY OF THE INVENTION

In consideration of the above circumstances, an objective of the present invention is to provide a system and method for preventing illegal use of software, which cannot be analyzed by using a software debugger which operates in any mode, and secret information stored in which cannot be retrieved even if backup data of the secret information is stored in another device.

Therefore, the present invention provides a system for preventing illegal use of software, comprising:

secret information storage means for storing secret information;

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;

illegal access determining means for determining whether an illegal access to the system is performed; and

cryptosystem key updating means for:

providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;

providing different keys for the above two kinds of cryptosystem keys if the illegal access determining means detects an illegal access; and

wherein the cryptosystem key updating means updates the above two kinds of cryptosystem keys for each access to the system.

The present invention also provides a method and a storage medium storing a computer-executable program, which correspond to the above system.

In the present invention, the illegal access determining means (for detecting an illegal operation) is provided. If an illegal user who accesses the system tries to decrypt the secret information stored in the secret information storage means, the secret information cannot be accurately decrypted, while a legal user who accesses the system can decrypt the encrypted secret information stored in the secret information storage means by performing a specific operation necessary for the decryption. That is, from the second access, the secret information cannot be decrypted, and it is possible to

prevent an illegal user from retrieving secret information used in a software by analyzing the system by using a software debugger or by falsifying the software.

In addition, the secret information storage means and the cryptosystem key storage means may be separately constructed. In this case, backup data of the secret information and the cryptosystem key can be stored, for example, in different file storage devices. As different cryptosystem keys are provided by the cryptosystem key updating means when an illegal operation is detected, even if an illegal user restores the secret information after the system becomes abnormal due to an illegal operation, normal operation using correct secret information becomes impossible.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing the system arrangement as an embodiment according to the present invention.

Fig. 2 is a flowchart showing the operations of the embodiment.

Fig. 3 is a diagram explaining the operations executed when normal access is performed.

Fig. 4 is a diagram explaining the operations executed when illegal access is attempted by an illegal user.

Fig. 5 is a block diagram showing an example of the conventional system for preventing illegal use of software.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hereinafter, an embodiment of the present invention will be explained with reference to the drawings.

(1) Structure of the embodiment

Fig. 1 is a block diagram showing the structure of the system for preventing illegal use of software in the present embodiment.

As shown in Fig. 1, the system of the present embodiment comprises program-controlled data processor 100, and file storage devices 110 and 113.

The data processor 100 includes illegal operation detecting unit 101 functioning as the illegal access determining means of the present invention, cryptosystem key readout unit 102, cryptosystem key updating unit 103, cryptosystem key storing unit 104, decrypting unit 105, and encrypting unit 106. The operations of these units will be explained later.

The file storage device 113 includes secret information storage unit 112 for storing encrypted secret information, and the file storage device 110 includes cryptosystem key storage unit 111 for storing a cryptosystem key necessary for decrypting the encrypted secret information stored in the secret information storage unit 112. Here, the cryptosystem key storage unit 111 and the secret information storage unit 112 are respectively stored in different file storage devices so as to prevent an illegal user from retrieving the cryptosystem key and the secret information in a single operation. That is, in the present system, two backup operations are necessary for storing backup data of the cryptosystem key and the secret information.

The operations of the above units 101 to 106 will be explained below.

The illegal operation detecting unit 101 detects whether an illegal user who wants secret information (for example, a secret key used in a secret-key cryptosystem or an encrypting algorithm itself) tries to read out the secret information (the practical method will be explained later). If it is detected that such an illegal try is performed, the illegal operation detecting unit 101 informs the cryptosystem key updating unit 103 (explained below) of the detected result.

The cryptosystem key readout unit 102 reads out cryptosystem key *a* for decrypting secret information from the cryptosystem key storage unit 111.

The cryptosystem key updating unit 103 updates the cryptosystem key in a specific operation depending on the situation (explained below), and sends the updated key to the cryptosystem key storing unit 104 and the encrypting unit 106.

That is, if an illegal try for reading out the secret information has been detected by the illegal operation detecting unit 101, the cryptosystem key updating unit 103 sends completely different cryptosystem keys *b* and *c* to the cryptosystem key storing unit 104 and the encrypting unit 106 (i.e., cryptosystem key $b \neq$ cryptosystem key *c*). In the normal operation (when no illegal try for reading out the secret information is performed), the cryptosystem key updating unit 103 sends the same key as the cryptosystem keys *b* and *c*, to the cryptosystem key storing unit 104 and the encrypting unit 106 (i.e., cryptosystem key $b =$ cryptosystem key *c*).

The cryptosystem key storing unit 104 stores the new cryptosystem key *b*, updated by the cryptosystem key updating unit 103, into the cryptosystem key storage unit 111.

The decrypting unit 105 reads out the encrypted secret information from the secret information storage unit 112, and decrypts the secret information using the cryptosystem key *a* read out by the cryptograph-key readout unit 102 so as to obtain the secret information necessary for performing specific operations of the system.

The encrypting unit 106 reencrypts the secret information (decrypted by the decrypting unit 105) by using new cryptosystem key *c* updated by the cryptosystem key updating unit 103, and stores the reencrypted secret information into the secret information storage unit 112.

(2) Operation

the operations of the present embodiment will be explained in detail with reference to the above Fig. 1 and the flowchart shown in Fig. 2.

First, cryptosystem key readout unit 102 reads out cryptosystem key *a* from the cryptosystem key storage unit 111 (see step A1 in Fig. 2).

Next, illegal operation detecting unit 101 detects whether an illegal user who wants secret information tries to read out the secret information (see step A2). In this detection, for example, it is examined whether an illegal user falsifies the present system (for preventing illegal use of software) operating in the data processor 100. Such an examination is performed by, for example, detecting a falsifying operation using electronic signatures and secret-key encryption. Simultaneously, a program-analyzing operation using a software debugger is also detected.

The cryptosystem key updating unit 103 updates the cryptosystem key for reencrypting the secret information (see step A3 or A4).

That is, if no illegal operation is detected by the illegal operation detecting unit 101 in step A2 (i.e., the detection result is "NO"), the cryptosystem key updating unit 103 provides the same key for (i) cryptosystem key *b* stored by the cryptosystem key storing unit 104 into the cryptosystem key storage unit 111 and (ii) cryptosystem key *c* used by the encrypting unit 106 for reencrypting the secret information (i.e., cryptosystem key *b* = cryptosystem key *c*) (see step A3).

On the other hand, if an illegal operation is detected in step A2 (i.e., the detection result is "YES"), the cryptosystem key updating unit 103 provides completely different keys as cryptosystem keys *b* and *c* (i.e., cryptosystem key *b* ≠ cryptosystem

key *c*) (see step A4).

In the cryptosystem-key updating operation performed by the unit 103, a one-direction function or a pseudo-random number is used for generating a new cryptosystem key so that cryptosystem keys *a* and *c* are not easily calculated or determined with reference to cryptosystem key *b*.

The decrypting unit 105 reads out the encrypted secret information from the secret information storage unit 112, and decrypts the information using the cryptosystem key *a* read out by the cryptosystem key readout unit 102 so that non-encrypted original secret information is retrieved (see step A5). Therefore, an operation using the secret information, such as a transaction-authenticating operation using the secret-key encryption, is performed (see step A6).

The encrypting unit 106 reencrypts the secret information, which was decrypted by the decrypting unit 105, by using the cryptosystem key *c* updated by the cryptosystem key updating unit 103 (see step A7), and stores the reencrypted secret information into the secret information storage unit 112 (see step A8).

The cryptosystem key storing unit 104 stores the cryptosystem key *b* updated by the cryptosystem key updating unit 103 into the cryptosystem key storage unit 111 (see step A9).

(3) Example

Below, an example according to the present embodiment will be explained with reference to Figs. 3 and 4.

(3-1) When no illegal try is performed:

Fig. 3 is a diagram explaining the operations executed when no illegal try is

performed by an illegal user.

As shown in Fig. 3, initial cryptosystem key *a1* (whose code (value) is "01010101") may be stored in the cryptosystem key storage unit 111, and secret information encrypted using the cryptosystem key *a1* is stored in the secret information storage unit 112. Here, the code length of the cryptosystem key is 8 bits for ease of explanation. However, actually, a key consisting of a much longer code (generally, a few ten to a few thousand of bits) is used according to the strength of the encryption algorithm.

In step A1 in the first execution, the cryptosystem key readout unit 102 reads out cryptosystem key *a1* from the cryptosystem key storage unit 111. Here, no illegal try is detected in step A2; thus, new cryptosystem keys *b1* and *c1* (which were updated in step A3) are the same (i.e., "10111000"), as described above (i.e., cryptosystem key *b1* = cryptosystem key *c1*). The decrypting unit 105 decrypts the secret information using the first cryptosystem key *a1* (see step A5). The encrypting unit 106 reencrypts the decrypted secret information by using updated cryptosystem key *c1* ("10111000") (see step A7). In addition, the cryptosystem key storing unit 104 stores the updated cryptosystem key *b1* ("10111000") into the cryptosystem key storage unit 111 (see step A9).

In step A1 in the second execution, the cryptosystem key readout unit 102 reads out cryptosystem key *b1* (= cryptosystem key *a2*: "10111000") which was stored into the cryptosystem key storage unit 111 in the step S9. The decrypting unit 105 decrypts the encrypted secret information (stored in the secret information storage unit 112) by using this cryptosystem key *a2* (see step A5). The secret information to be decrypted was encrypted in the first execution by using cryptosystem key *c1* (= cryptosystem key *b1*:

"10111000"). As the cryptosystem keys *a2* and *c1* have the same code value ("10111000"), the decrypting operation is accurately performed so that correct secret information can be obtained.

Similar operations are performed from the third execution and the cryptosystem key for encrypting the secret information is updated for each execution, and correct secret information can be obtained in each execution.

(3-2) When an illegal try is performed:

Fig. 4 is a diagram explaining the operations executed when an illegal try is performed by an illegal user.

As shown in Fig. 4, initial cryptosystem key *a1* (whose code (value) is "01010101") may be stored in the cryptosystem key storage unit 111, and secret information encrypted using the cryptosystem key *a1* is stored in the secret information storage unit 112.

In step A1 in the first execution, the cryptosystem key readout unit 102 reads out cryptosystem key *a1*. Here, an illegal try is detected in step A2; thus, new cryptosystem keys *b1* and *c1* (which were updated in step A3) have different code values (i.e., "10111000" and "11100101") (i.e., cryptosystem key *b1* $\neq$ cryptosystem key *c1*).

The decrypting unit 105 decrypts the secret information using the first cryptosystem key *a1* (see step A5). The encrypting unit 106 reencrypts the decrypted secret information by using the updated cryptosystem key *c1* ("11100101") (see step A7). In addition, the cryptosystem key storing unit 104 stores the updated cryptosystem key *b1* ("10111000") into the cryptosystem key storage unit 111 (see step A9).

In step A1 in the second execution, the cryptosystem key readout unit 102 reads

out cryptosystem key *a2* ("10111000"). The decrypting unit 105 decrypts the secret information, stored in the cryptosystem key storage unit 111, by using this cryptosystem key *a2* (see step A5). The secret information to be decrypted was encrypted in the first execution by using the cryptosystem key *c1* ("11100101"). Here, cryptosystem keys *a2* and *c1* have different code values ("10111000" and "11100101"); thus, decryption cannot be accurately performed and the obtained secret information is not correct.

In order for an illegal user to obtain correct secret information after this phase, the illegal user must know the code value "11100101" of the cryptosystem key *c1*. As this value is not stored in the file storage unit 110, it is necessary to try any possible value for the cryptosystem key. The above illegal-use preventing method can have an effect or strength sufficient for practical use though it depends on the encrypting algorithm and the code length of the key.

Before the first execution, the secret information which was encrypted by the cryptosystem key *a1* ("01010101") stored in the cryptosystem key storage unit 111 may be stored in another file storage device as backup data in advance. However, in the above situation in which the obtained secret information is not correct, even though the encrypted secret information can be restored, it is difficult to retrieve the correct secret information because the code value of the cryptosystem key *a1* is lost in this phase.

If the code value of cryptosystem key *a1* stored in the cryptosystem key storage unit 111 is also stored in another file storage device before the first execution, the retrieval of the secret information is not impossible. However, such a detailed system structure can be known by an illegal user only via an illegal analysis using a software debugger (that is, via an illegal try detected by the illegal-operation detecting unit 101).

From the third execution (of the steps in the flowchart of Fig. 2), similar operations are performed and the correct secret information cannot be obtained. When

such execution is repeated, encrypting and decrypting operations are performed using a different cryptosystem key for each execution; thus, retrieval of the secret information becomes very difficult.

The present invention is suitably applicable to IC cards which are distributed to many persons in general. In another application, the present invention can be used when distributing software or microcomputers (such as semiconductor integrated circuits) using secret information (a secret key for authentication) which relate to electronic transactions and thus should be secret to third parties.

EP 0 955 747 A2

What is claimed is:

1. A system for preventing illegal use of software, comprising:

secret information storage means for storing secret information;

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means;

illegal access determining means for determining whether an illegal access to the system is performed; and

cryptosystem key updating means for:

providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access;

providing different keys for the above two kinds of cryptosystem keys if the illegal access determining means detects an illegal access; and

wherein the cryptosystem key updating means updates the above two kinds of cryptosystem keys for each access to the system.

2. A method for preventing illegal use of software, the method used in a system which comprises a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the method comprising the steps of:

determining whether an illegal access to the system is performed; and

for each access to the system,

providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.

3. A storage medium storing a computer-executable program for preventing illegal use of software, the program used in a system which comprises a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the program including the processes of:

determining whether an illegal access to the system is performed; and

for each access to the system,

providing the same updated key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed;

providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed.

4. A system for preventing illegal use of software as claimed in claim 1, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

5. A method for preventing illegal use of software as claimed in claim 2, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

6. A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the secret information storage means and the cryptosystem key storage means are separately constructed.

7. A system for preventing illegal use of software as claimed in claim 1, wherein the system is applied to an IC card.

8. A method for preventing illegal use of software as claimed in claim 2, wherein the system in which the method is used is applied to an IC card.

9. A storage medium storing a computer-executable program for preventing illegal use of software as claimed in claim 3, wherein the system in which the program is used is applied to an IC card..

ABSTRACT

A system and method for preventing illegal use of software is provided, which cannot be analyzed by using a software debugger which operates in any mode, and the secret information stored in which cannot be retrieved even if backup data of the secret information is stored in another device. The system comprises a unit for storing secret information; a unit for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means; a unit for determining whether an illegal access to the system is performed; and a cryptosystem key updating unit for providing the same key for a cryptosystem key used for reencrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if the illegal access determining means detects no illegal access, or providing different keys for the above two kinds of cryptosystem keys if the illegal access determining means detects an illegal access, and wherein the cryptosystem key updating units updates the above two kinds of cryptosystem keys for each access to the system.

FIG.1

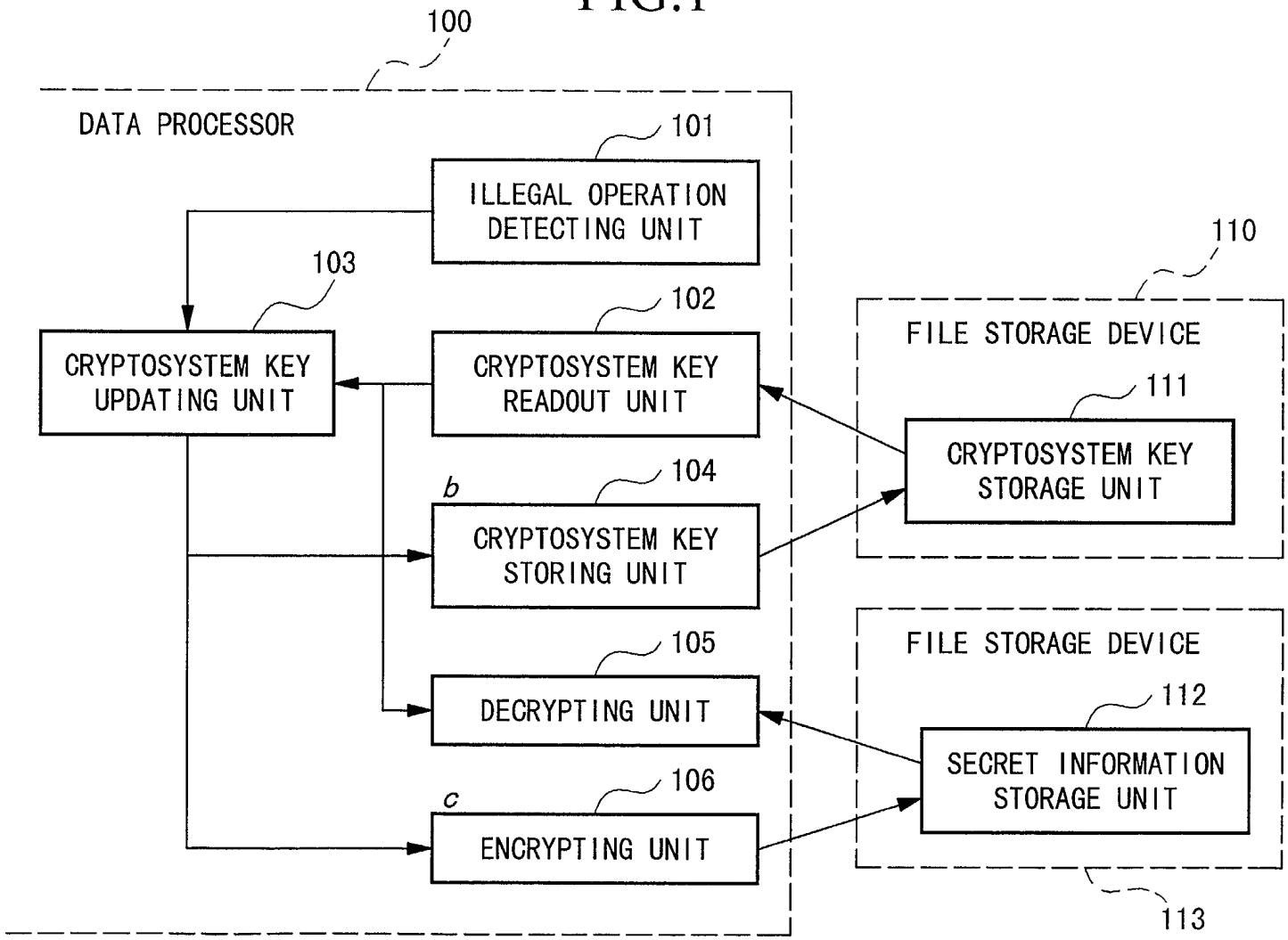

100
DATA PROCESSOR
101
ILLEGAL OPERATION DETECTING UNIT
103
CRYPTOSYSTEM KEY UPDATING UNIT
102
CRYPTOSYSTEM KEY READOUT UNIT
b
104
CRYPTOSYSTEM KEY STORING UNIT
105
DECRYPTING UNIT
c
106
ENCRYPTING UNIT
110
FILE STORAGE DEVICE
111
CRYPTOSYSTEM KEY STORAGE UNIT
FILE STORAGE DEVICE
112
SECRET INFORMATION STORAGE UNIT
113

FIG.2

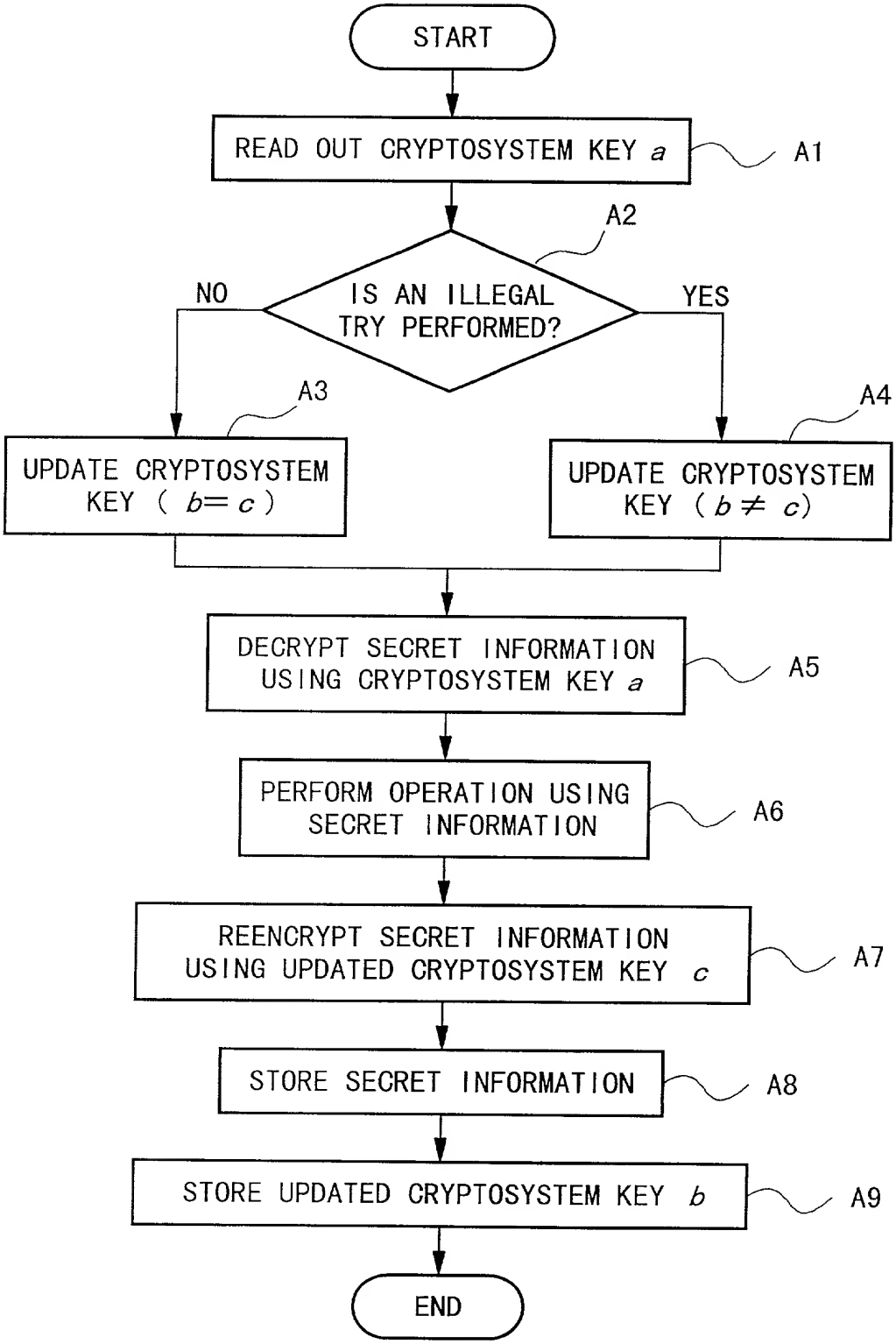

START
READ OUT CRYPTOSYSTEM KEY a
A1
A2
IS AN ILLEGAL TRY PERFORMED?
NO
YES
A3
A4
UPDATE CRYPTOSYSTEM KEY (b= c)
UPDATE CRYPTOSYSTEM KEY (b ≠ c)
DECRYPT SECRET INFORMATION USING CRYPTOSYSTEM KEY a
A5
PERFORM OPERATION USING SECRET INFORMATION
A6
REENCRYPT SECRET INFORMATION USING UPDATED CRYPTOSYSTEM KEY c
A7
STORE SECRET INFORMATION
A8
STORE UPDATED CRYPTOSYSTEM KEY b
A9
END

FIG.3

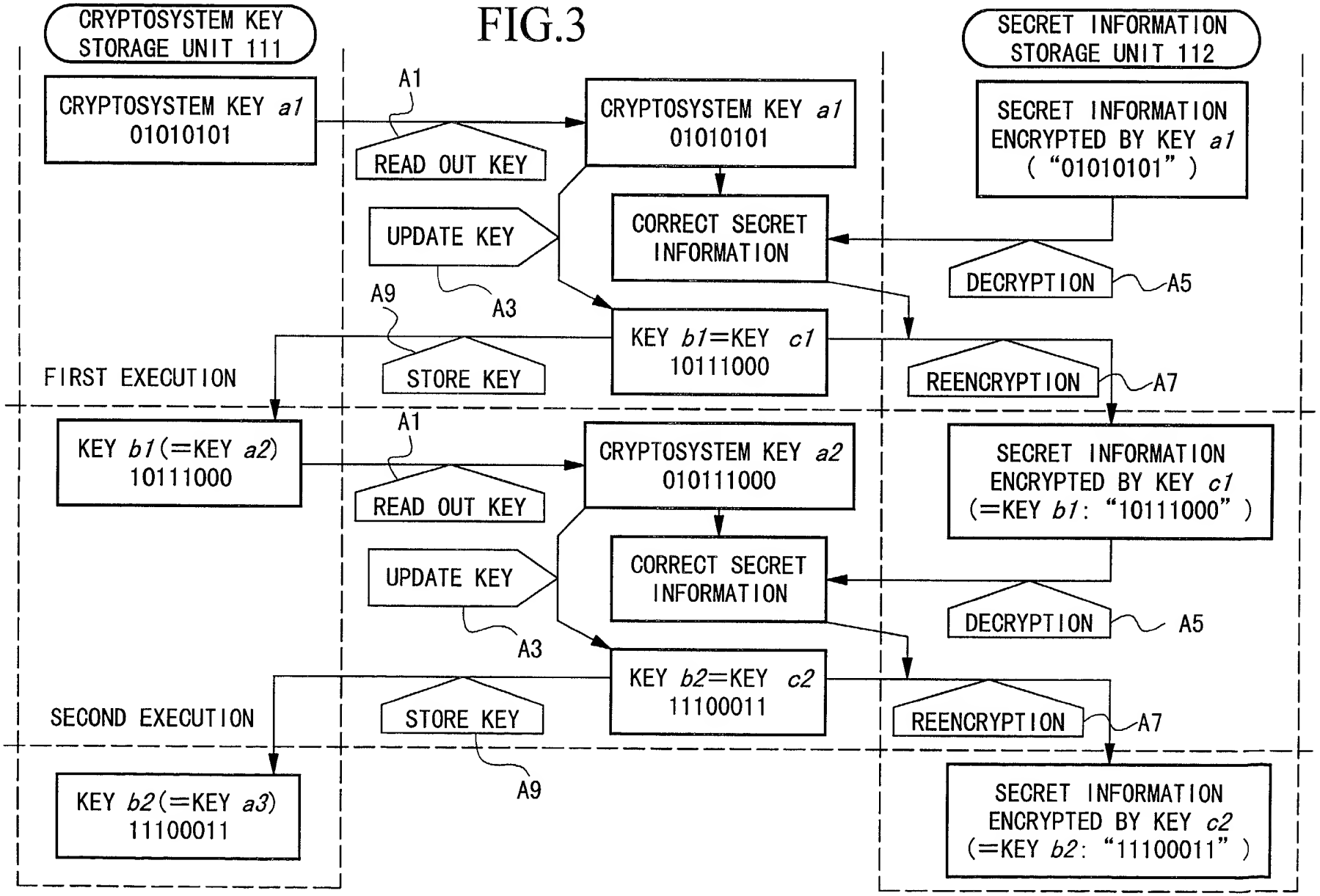

CRYPTOSYSTEM KEY STORAGE UNIT 111
SECRET INFORMATION STORAGE UNIT 112
CRYPTOSYSTEM KEY a1 01010101
A1
READ OUT KEY
CRYPTOSYSTEM KEY a1 01010101
SECRET INFORMATION ENCRYPTED BY KEY a1 ("01010101")
UPDATE KEY
A3
CORRECT SECRET INFORMATION
DECRYPTION
A5
A9
STORE KEY
KEY b1=KEY c1 10111000
REENCRYPTION
A7
FIRST EXECUTION
KEY b1(=KEY a2) 10111000
A1
READ OUT KEY
CRYPTOSYSTEM KEY a2 010111000
SECRET INFORMATION ENCRYPTED BY KEY c1 (=KEY b1: "10111000")
UPDATE KEY
A3
CORRECT SECRET INFORMATION
DECRYPTION
A5
KEY b2=KEY c2 11100011
STORE KEY
A9
REENCRYPTION
A7
SECOND EXECUTION
KEY b2(=KEY a3) 11100011
SECRET INFORMATION ENCRYPTED BY KEY c2 (=KEY b2: "11100011")

FIG.4

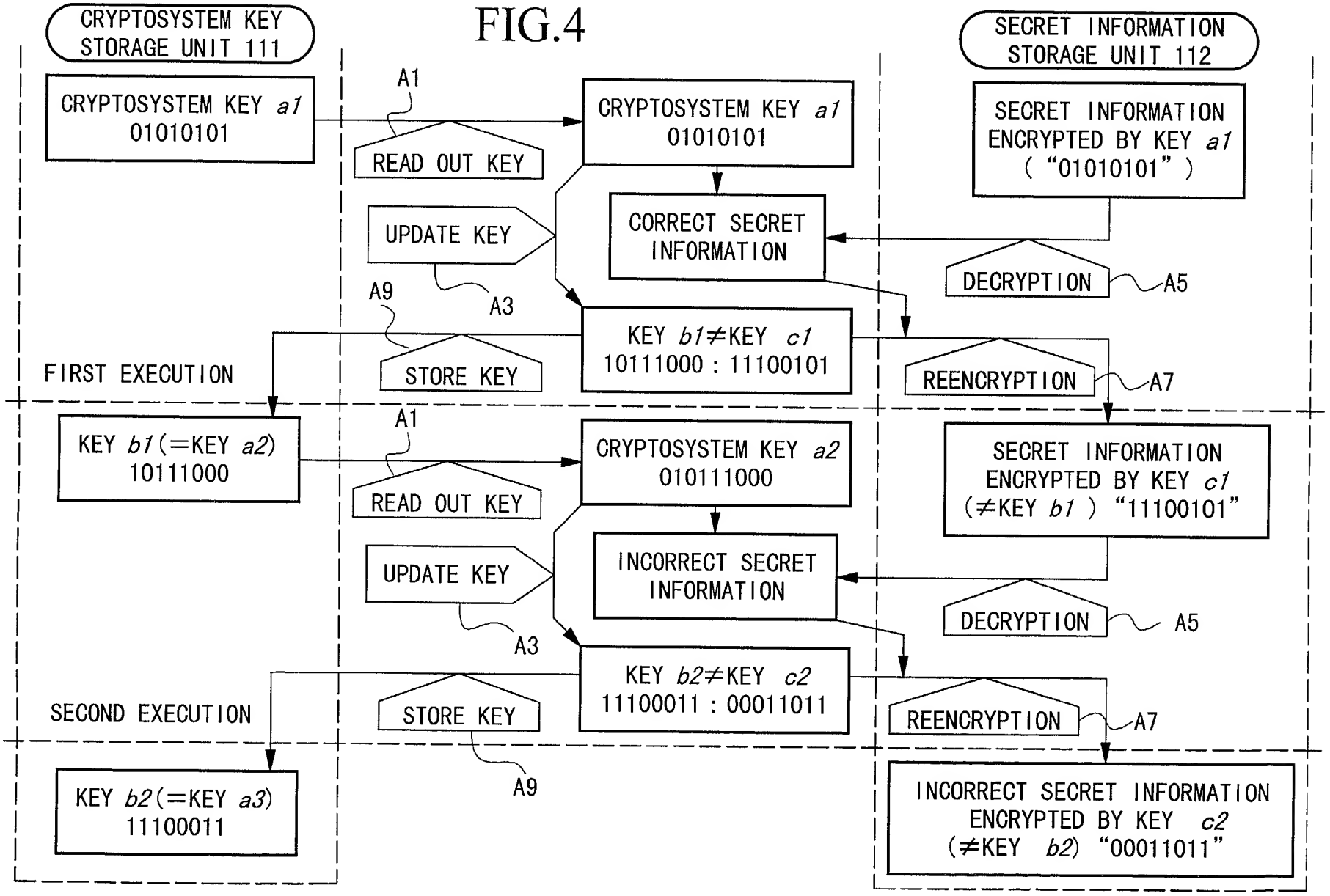
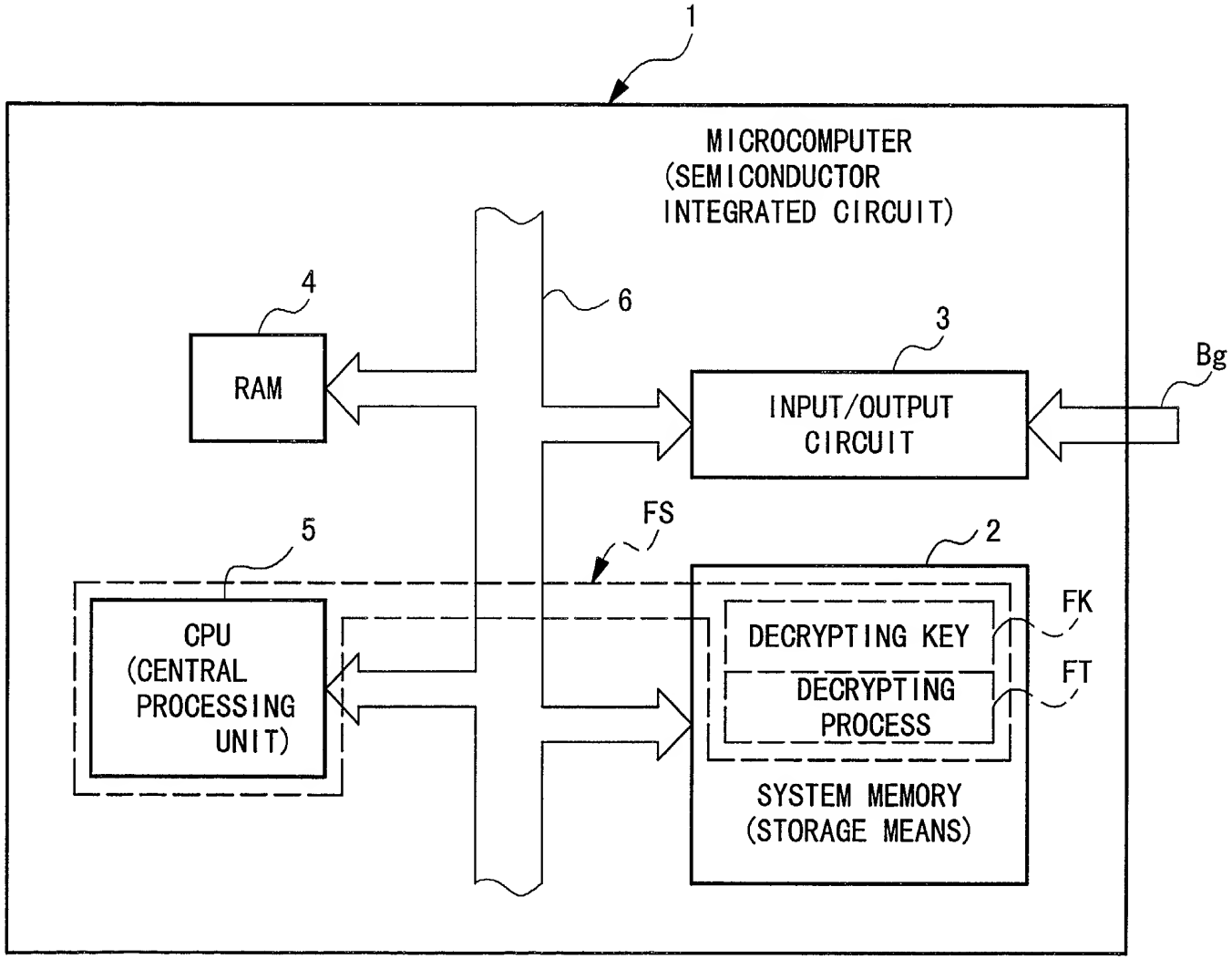

CRYPTOSYSTEM KEY STORAGE UNIT 111
SECRET INFORMATION STORAGE UNIT 112
CRYPTOSYSTEM KEY a1 01010101
A1
READ OUT KEY
CRYPTOSYSTEM KEY a1 01010101
SECRET INFORMATION ENCRYPTED BY KEY a1 ("01010101")
UPDATE KEY
A3
CORRECT SECRET INFORMATION
DECRYPTION
A5
A9
STORE KEY
KEY b1≠KEY c1 10111000 : 11100101
REENCRYPTION
A7
FIRST EXECUTION
KEY b1(=KEY a2) 10111000
A1
READ OUT KEY
CRYPTOSYSTEM KEY a2 010111000
SECRET INFORMATION ENCRYPTED BY KEY c1 (≠KEY b1) "11100101"
UPDATE KEY
A3
INCORRECT SECRET INFORMATION
DECRYPTION
A5
KEY b2≠KEY c2 11100011 : 00011011
STORE KEY
A9
REENCRYPTION
A7
SECOND EXECUTION
KEY b2(=KEY a3) 11100011
INCORRECT SECRET INFORMATION ENCRYPTED BY KEY c2 (≠KEY b2) "00011011"

FIG.5


1
MICROCOMPUTER
(SEMICONDUCTOR
INTEGRATED CIRCUIT)
4
RAM
6
3
INPUT/OUTPUT
CIRCUIT
Bg
5
CPU
(CENTRAL
PROCESSING
UNIT)
FS
2
DECRYPTING KEY
FK
DECRYPTING
PROCESS
FT
SYSTEM MEMORY
(STORAGE MEANS)

10-125619 OSP-7978

Docket No _____ 2-1

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR PREVENTING ILLEGAL USE OF SOFTWARE

the specification of which is attached hereto unless the following box is checked:

☐ was filed on _____ as United States Application Number or PCT International Application Number _____ and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

NUMBER	COUNTRY	DAY/MONTH/YEAR FILED	PRIORITY CLAIMED
Patent 10-125619	Japan	08/05/1998	Yes

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

APPLICATION NO.	FILING DATE

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is known by me to be material to patentability as defined in Title 37, Code of Federal Regulations § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS: PATENTED, PENDING, ABANDONED

I hereby appoint as my attorneys, with full powers of substitution and revocation, to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Stephen A. Bent, Reg. No. 29,768; David A. Blumenthal, Reg. No. 26,257, John J. Feldhaus, Reg. No. 28,822; Donald D. Jeffery, Reg. No. 19,980; Eugene M. Lee, Reg. No. 32,039; Peter G. Mack, Reg. No. 26,001; Brian J. McNamara, Reg. No. 32,789; Sybil Meloy, Reg. No. 22,749; George E. Quillin, Reg. No. 32,792; Colin G. Sandercock, Reg. No. 31,298; Bernhard D. Saxe, Reg. No. 28,665; Charles F. Schill, Reg. No. 27,590; Richard L. Schwaab, Reg. No. 25,479; Arthur Schwartz, Reg. No. 22,115; Harold C. Wegner, Reg. No. 25,258.

Address all correspondence to FOLEY & LARDNER, Washington Harbour, 3000 K Street, N.W., Suite 500, P.O. Box 25696, Washington, D.C. 20007-8696. Address telephone communications to _____ at (202) 672-5300.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First or Sole Inventor	Signature of First or Sole Inventor	Date
Takuya Morishita	Takuya Morishita	April 21, 1999
Residence Address		**Country of Citizenship**
Tokyo, Japan		Japan
Post Office Address		
c/o NEC Corporation, 7-1, Shiba 5-chome, Minato-ku, Tokyo, Japan		

Full Name of Second Inventor	Signature of Second Inventor	Date
Residence Address		**Country of Citizenship**
Post Office Address		

Full Name of Third Inventor	Signature of Third Inventor	Date
Residence Address		**Country of Citizenship**
Post Office Address		

Full Name of Fourth Inventor	Signature of Fourth Inventor	Date
Residence Address		**Country of Citizenship**
Post Office Address		

Full Name of Fifth Inventor	Signature of Fifth Inventor	Date
Residence Address		**Country of Citizenship**
Post Office Address		